

'Exciting Transformation' Underway in System Assurance Engineering

By Christopher Dauer IDGA Editor

Successful mission assurance depends on successful system assurance, which requires a balance of security and compliance—and the nature of that balance has started to evolve in a dramatic fashion.

"It's an exciting transformation," according to Harrell J. Van Norman, ASIP ISSM, AFMC/ASC/WIN. The Air Force Materiel Command's Aeronautical Systems Center designs, develops and delivers dominant aerospace weapon systems and capabilities for U.S. Air Force, other U.S. military, allied and coalitionpartner warfighters, in support of Air Force leadership priorities. Mr. Van Norman's current role is as Information System Security Manager for AF UAV sensor systems, participating on the System Assurance, Platform Information Technology, and Cyber Security working groups.

Security is now being viewed from a comprehensive risk management perspective, he said. But first, he noted that it's important to understand that mission assurance is largely a function of combining levels of system assurance.

"Few people can focus on mission assurance, because few people have jurisdiction over the entire mission," he said. "I do system assurance. If everybody focuses on their system, the mission will follow."

System assurance, explained Mr. Van Norman, is an integration of multiple disciplines and multiple aspects of security. The overall system is full of vulnerabilities, which can be introduced in a number of times throughout its lifecycle. So there are anti-tampering controls, along with hardware and software assurance issues, that all come together for system assurance.

The key change now is a shift away from a focus on legal or regulatory compliance, and a move to genuine security. "The question is, is the system really safe, or are we just trying to meet a legal or certification requirement?" he asked. To illustrate, Mr. Van Norman drew a parallel to driving safety.

"You drive down the highway, and the sign says the speed limit is 35 miles per hour. Are you focused on that, or are you focused on driving safely? There could be other issues—you could be texting!—so that

you wouldn't really be driving safely," he said. "Or, when you get your driver's license—its gives you the right to drive a car—or in this case operate a system— but you still have to drive safely. That's what we're trying to shift to, and it's an exciting transformation. We're moving toward a concept of continuous monitoring."

Periodic formalized reviews are no substitute for this kind of ongoing monitoring, he said, drawing a parallel to cell phones of today to their "radically different" counterparts five years ago. "We need continual assessment to understand current and future threats and vulnerabilities," he said.

For example, the primary area of attack has shifted from perimeter-based vulnerabilities to software operating the systems.

"Think of Mr. McGregor's garden, and how he tried to keep the rabbits away," said Mr. Van Norman, referring to the tale of Peter Rabbit. "They'd burrow under his fence, so he'd build a big deep fence. So, because he fixed that attack vector, they might go over the fence, so he addressed that. It's all about addressing different attack vectors."

Effective security requires a host of processes, including static source code analysis and dynamic source code analysis, he said, noting that successful mission assurance "is a constant war of cyber-security. And it really is a war."

Harrell J. Van Norman, ASIP ISSM, AFMC/ASC/WIN will be speaking at IDGA's Mission Assurance and Information Security Summit, to be held from Feb. 15-17, 2012 in Washington, DC. For more information on the conference, visit <u>www.missionassurancesummit.com</u>, or call 1-800-882-8684.